Implicaciones financieras de la implantación de ISO/IEC 27001 & 27002: modelo genérico de coste-beneficio

Gary Hinson, IsecT Ltd., 15th January 2008
Traducido por: iso27000.es

Resumen Ejecutivo

Beneficios

- Reduce los riesgos de seguridad de la información. Reduce la probabilidad y el impacto de los incidentes de seguridad
- La certificación de un estándar internacional. Ventajas de marketing, etc.
- Enfoque coherente, estructurado. Evaluación integral de riesgos
- Focaliza el gasto en seguridad de la información donde produce mayor ventaja.
- Gobernanza demostrable

Costes

- Gestión de proyectos, recursos del proyecto
- El cambio organizacional requiere recursos de la organización
- Diseño, desarrollo, pruebas, implementación
- Certificación y visitas de seguimiento
- Operación y mantenimiento en curso

Introducción

Las organizaciones que intentan adoptar la norma ISO/IEC 27002 (estándar internacional de código de buenas prácticas para la gestión de seguridad de la información) e ISO/IEC 27001 (estándar para la certificación del sistema de gestión de seguridad de la información) suelen organizar el trabajo asociado como un proyecto de implementación. Este modelo financiero genérico descrito en este documento explica las consecuencias financieras de la aplicación de las normas ISO/IEC 27001 y 27002 como un conjunto de beneficios típicos y categorías de los costes. El modelo puede ser utilizado tanto como base para justificar el proyecto a la alta dirección como un caso de negocio, como para marco para medir y optimizar el valor neto de la inversión a largo plazo.

Beneficios

Reduce los riesgos de seguridad de la información

- Fortalece la seguridad de la información en el entorno actual al (re)hacer hincapié en los requisitos de control de la seguridad de la información de negocio, actualización de las actuales políticas de seguridad de la información, controles, etc. y proporcionar estímulo para revisar y actualizar periódicamente los controles de seguridad de la información - **reducción del riesgo.**
- De manera integral y exhaustiva reduce la probabilidad de amenazas a la información de seguridad o vulnerabilidades no reconocidas - **reducción del riesgo.**
- Enfoque de gestión de riesgos profesional, normalizado y racional que aporta consistencia a través de múltiples (todos!) sistemas en el tiempo, y aborda los riesgos de seguridad de la información de forma consistente (el enfoque basado en el riesgo se centra en las áreas de mayor riesgo) - **reducción del riesgo**
- Aumenta la capacidad de transferir los riesgos de manera selectiva a las aseguradoras y permite la negociación para reducir las primas de seguros mediante los controles que se implementan - **ahorro de costes**
- Administradores y personal estarán cada vez más familiarizados con los términos y los controles de seguridad de la información - **reducción del riesgo**

Beneficios de la estandarización

- Proporciona un "denominador común": una sólida base sobre la que construir controles adicionales específicos del sistema según sea apropiado sin tener que revisar constantemente los controles básicos - **ahorro de costes**
- Evita la necesidad de especificar, aplicar y revisar por separado los requisitos básicos de referencia para el control y los controles en cada sistema - **ahorro de costes**
- Es de aplicación general y por tanto, directamente reutilizable a través de diversos departamentos, funciones y organizaciones sin cambios relevantes - **ahorro de costes**
- Permite a la organización concentrar sus esfuerzos y recursos en identificar y satisfacer requisitos por encima de los básicos de control - **ahorro de costes**
- Generalmente aceptadas y bien establecidas (BS 7799 → ISO/IEC 17799 → ISO/IEC 27002) con un incremento en la concienciación y aceptación a nivel mundial
- Buenas prácticas reconocidas y aceptadas en seguridad de la información - ¿por qué reinventar la rueda? - **ahorro de costes**
- Ahorra tiempo y dinero mediante la adopción directa de buenas prácticas - **ahorro de costes**
- Proporciona una terminología común para discutir, especificar, desarrollar y evaluar las necesidades en seguridad de la información y los controles
- Permite incluso relajar la aplicación de algunos controles - **ahorro de costes**

Beneficios de disponer de un enfoque estructurado

- ISO/IEC 27002 es un marco lógico para diferentes controles de seguridad de la información y constituye una base racional para evaluar los riesgos y la aplicación de controles adecuados. Es internamente consistente y razonablemente coherente sin llegar a ser excesivamente prescriptivo (especialmente si los usuarios se centran en los objetivos de control más amplios). Es personalizable y constituye una buena base sobre la que construir extensiones específicas para la organización o de la industria según sea necesario **- beneficios generales**

- Proporciona el impulso necesario para revisar los sistemas, datos y flujos de información con el potencial para reducir la sobrecarga de duplicidades y otros sistemas/datos/procesos innecesarios y mejorar la calidad de la información (re-ingeniería de los procesos de negocio) **- ahorro de costes**
- Proporciona un mecanismo para medir el rendimiento y aumentar gradualmente la línea base de referencia para la seguridad de la información **- los beneficios a largo plazo**
- Después de haber aplicado las normas ISO/IEC 27001 y 27002, la organización tendrá un amplio conjunto de políticas y procedimientos de seguridad de la información formalmente aprobado que serán más fáciles de seguir por parte del personal y los gerentes coherentemente **- los beneficios a largo plazo**

Beneficios de la certificación

- Satisfacer las peticiones de partners y proveedores para justificar los controles de seguridad de la información sin necesidad de atender consultas individuales o proporcionar información confidencial **- ahorro de costes y reducción de riesgos**
- Proporciona un estándar de seguridad de la información racional e independiente con el que evaluar la calidad de los controles en partners y proveedores **- ahorro de costes y reducción de riesgos**
- Potencialmente, ofrece una ventaja de marketing en los primeros en adoptar la certificación ("insignia de honor" similar a la norma ISO 9000 de calidad) **– beneficios en marketing/ventas**
- La resistencia a demostrar el cumplimiento de la normas ISO/IEC 27001/2 puede ser tomado como un signo de vulnerabilidad. Certificar el cumplimiento puede promover la imagen de la empresa como un socio seguro para los negocios **- ventaja competitiva**
- Ayuda a garantizar a las partes interesadas, los auditores, los reguladores de la industria, etc. que la organización está activamente minimizando los riesgos de seguridad de la información mediante la demostración del compromiso de la organización en seguridad de la información (gobierno corporativo o aspectos debidos a diligencia que aporten potenciales exposiciones a riesgos de la seguridad de la información) **- ahorro de costes y reducción de riesgos**

Evitar Costes

- La organización puede verse obligada a acometer este camino eventualmente en cualquier circunstancia y por las presiones del mercado, especialmente si desde otras partes interesadas comienzan a exigir el cumplimiento de la norma ISO/IEC 27002 o de certificación de ISO/IEC 27001 como prerrequisito para eCommerce, etc. Mediante una implantación dentro de las propias escalas de tiempo las organizaciones pueden elegir la secuencia de acciones más eficaz en costes **- reducción de costos**
- Los gobiernos y reguladores de la industria pueden insistir en el cumplimiento de la norma ISO/IEC 27002 como regla habitual. Puede que sea necesario demostrar el cumplimiento de la protección de datos y privacidad o similar legislación **- requisitos legales/reglamentarios para evitar sanciones**
- Potencialmente reduce o restringe las quejas de terceras partes en caso de fallos de seguridad de información **- ahorro de costes y reducción de riesgos**

Costes

Costes relacionados con los cambios organizacionales

- Necesidad de elevar la concienciación de la organización (personal y directivo)
- Adaptación/racionalización de las normas, procedimientos, prácticas, etc. vigentes de seguridad de la información
- Puede ser necesario "dejar que cierto personal se vaya" por no cumplir con las políticas, etc.

Costes de diseño & desarrollo

- Revisión y actualización de las normas, directrices, procedimientos, etc., vigentes de seguridad de la información
- Preparación de (algunas) nuevas normas, directrices, procedimientos, etc., de seguridad de información
- (Re) diseño de la arquitectura de los controles

Costes de la implementación

- Los costos únicos iniciales para actualizar y/o complementar diversos controles existentes para cumplir con la norma
- Costes de concienciación y formación

Costes de certificación

- Visitas de pre-certificación y de certificación iniciales por entidades de certificación acreditadas por la norma ISO/IEC 27001 (algunos miles de EUR)
- Riesgo de no alcanzar la certificación a la primera (cualquiera de los motivos que causó el fracaso representan ellos mismos riesgos inaceptables para seguridad de la información – retraso de la certificación más probable que un fracaso completo)
- Tiempo dedicado por el personal/dirección en las visitas anuales de seguimiento
- Recertificación trianual (examen más amplio en las áreas de revisión y, por lo tanto, impacto mayor aunque todavía relativamente menor)
- Todos estos costos se reducirán al mínimo todos si logramos una implementación de alta calidad a través de nuestros propios esfuerzos

Costes de Mantenimiento del SGSI en curso

- Revisión/mantenimiento anual de las políticas, directrices, procedimientos, etc, de seguridad de la información para mantener el cumplimiento con la norma
- Costes menores para mantener el registro (algunos pocos miles de EUR) - tal vez se puede reducir mediante la combinación de la certificación de la norma ISO/IEC 27001 con ISO 9000.

Conclusión

Le animamos a utilizar este documento genérico como base para su propio caso de negocio, utilizando datos y estimaciones reales de su organización para consolidar las cifras. En cualquier caso contacte con el autor (Gary@isect.com) o visite www.ISO27001security.com para más información y consejos de otros implantadores de ISO/IEC 27001/2. Buena suerte!

Copyright